What is claimed is:

1. A network reference model for use in configuring security software on a computer network, the network reference model comprising:
a database engine providing deduction;
a network information database associated with the database engine and providing a central repository for a configuration of hardware and software installed on the network; and
a security goal database associated with the database engine and describing uses that the hardware and software installed on the network may support.

2. The network reference model of claim 1, further comprising:
an event database associated with the database engine and containing events related to the network, wherein such events include possible attacks against the network and benign events that could be confused with the possible attacks.

3. The network reference model of claim 1, wherein the database engine is an object-oriented description logic database engine.

4. A configuration tool for use in configuring security software packages on a computer network, the configuration tool comprising:
a description logic database engine;
a network information database associated with the description logic database engine and providing a central repository for a configuration of hardware and software installed on the network;
a security goal database associated with the description logic database engine and providing security goals describing uses that the hardware and software of the network may support;
a first configuration module coupled to the description logic database engine for configuring intrusion blocking security software packages; and
a second configuration module coupled to the description logic database engine for configuring intrusion detecting security software packages;

wherein the first configuration module configures the intrusion blocking security software packages based on the configuration of the hardware and software installed on the network and the security goals; and

wherein the second configuration module configures the intrusion detecting security software packages based on the configuration of the hardware and software installed on the network and the security goals.

5. The configuration tool of claim 4, further comprising:

an event database associated with the description logic database engine and containing events related to the network.

6. The configuration tool of claim 5, wherein the events contained in the event database include possible attacks against the network and benign events that could be confused with the possible attacks.

7. The configuration tool of claim 4, further comprising:

a system hardening module coupled to the description logic database engine for automating a process of hardening the network.

8. The configuration tool of claim 7, wherein the system hardening module is context sensitive.

9. The configuration tool of claim 4, further comprising:

an audit configuration module coupled to the description logic database engine for probing the network for vulnerabilities.

10. A configuration tool for use in configuring security software packages on a computer network, the configuration tool comprising:

a description logic database engine;

a network information database associated with the description logic database engine and providing a central repository for a configuration of hardware and software installed on the network;

a security goal database associated with the description logic database engine and providing security goals describing uses that the hardware and software of the network may support;

an event database associated with the description logic database engine and containing events related to the network, wherein the events contained in the event database include possible attacks against the network and benign events that could be confused with the possible attacks;

a first configuration module coupled to the description logic database engine for configuring intrusion blocking security software packages;

a second configuration module coupled to the description logic database engine for configuring intrusion detecting security software packages;

a system hardening module coupled to the description logic database engine for automating a process of hardening the network; and

an audit configuration module coupled to the description logic database engine for probing the network for vulnerabilities;

wherein the first configuration module configures the intrusion blocking security software packages based on the configuration of the hardware and software installed on the network and the security goals;

wherein the second configuration module configures the intrusion detecting security software packages based on the configuration of the hardware and software installed on the network and the security goals; and

wherein the system hardening module is context sensitive.

11. A method for configuring a security software package installed on an individual network device, the method comprising:

using active inference in a database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device, wherein the individual network device is a member of the class of network devices; and

configuring the security software package using the one or more security goals.

12. The method of claim 11, wherein using active inference further comprises automatically classifying the individual network device based on an IP address, a

network topology or a service provided by the individual network device, and applying rules to the individual network device based on its classification.

13. The method of claim 11, wherein the database engine is an object-oriented description logic database engine.

14. The method of claim 11, wherein the security software package is selected from the group consisting of an intrusion blocking software package and an intrusion detecting software package.

10035034.050501

15. A method for configuring a security software package installed on an individual network device, the method comprising:
using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device, wherein the individual network device is a member of the class of network devices; and
configuring the security software package using the one or more security goals;
wherein the security software package is selected from the group consisting of an intrusion blocking software package and an intrusion detecting software package.

16. The method of claim 15, wherein using active inference further comprises automatically classifying the individual network device based on an IP address, a network topology and one or more services the individual network device provides, and applying rules to the individual network device based on its classification.

17. A method for configuring a security software package, the method comprising:
defining one or more security policies for a class of network devices, wherein the security software package is a service running on at least one network device of the class of network devices;
using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals;

using to database engine providing deduction to associate the one or more security goals with the at least one network device; and

configuring the security software package on the at least one network device using the one or more security goals.

18. A method for configuring security software packages, comprising:

generating a first database containing a configuration of hardware devices and software packages installed on a network, wherein the software packages include the security software packages;

defining classes of hardware devices installed on the network;

automatically classifying each of the hardware devices into one of the classes of hardware devices using a database engine providing deduction;

generating a second database containing first security goals;

decomposing the first security goals into second security goals for individual hardware devices using the database engine and the configuration of the hardware devices and the software packages installed on the network; and

configuring each of the security software packages using the second security goals.

19. The method of claim 18, wherein generating a second database containing first security goals further comprises generating a second database containing first security goals for each class of hardware devices.

20. The method of claim 19, wherein decomposing the first security goals into second security goals for individual hardware devices further comprises using inference to associate the second security goals with individual hardware devices within each class of hardware devices.

10038.05435960